ABSTRACT

The present invention describes a network-based mobile workgroup system allowing a selected set of users from two or more mobile virtual private networks to form an extranet workgroup in a secure manner. The invention is based on the limited private address scenario, which entitles mobile nodes having private, possibly overlapping, addresses as defined in RFC 1918, while home and foreign agents have public IP addresses. Each home agent is dedicated to one mobile virtual private network (M-VPN), while a foreign agent may be shared by multiple M-VPNs. The system also entails a mobile service manager that has a public IP address and a set of mobile nodes that all have a UFQDN (user fully qualified domain name) within the overall mobile workgroup system.

The main benefits, compared to existing solution for extranet workgroup creation, are that extranets can be created despite overlapping address realms. Even fine-granular workgroups within the extranet can be created with any set of users from any set of M-VPNs. The mobility aspect of the M-VPN fits well for supporting peer-to-peer applications, such as voice over IP, between mobile clients. Although the mobile clients may belong to different M-VPNs, with different address realms, per packet authentication and filtering is always possible to perform by the ingress M-VPN security gateway using a realm-indexed filtering technique. Finally, the responsibility for allocating resources, to be reached by an extranet workgroup, is completely delegated to each M-VPN.